

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCHES OF
INFORMATION ASSOCIATED WITH:

(1) THE CELLULAR DEVICE ASSIGNED
CALL NUMBER **202-604-0663**, STORED AT
PREMISES CONTROLLED BY **VERIZON**
WIRELESS; and

Magistrate No. 20-293
UNDER SEAL

(2) THE CELLULAR DEVICE ASSIGNED
CALL NUMBER **202-840-4914**, STORED AT
PREMISES CONTROLLED BY **T-MOBILE**

Magistrate No. 20-294
UNDER SEAL

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR SEARCH WARRANTS

I, Ryan Melder, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for two search warrants for information associated with certain cellular telephones. Those telephones can be described as: (1) a telephone assigned call number **202-604-0663**, which information is stored at premises controlled by **VERIZON WIRELESS**, a wireless telephone service provider headquartered at 180 Washington Valley Road, Bedminster, NJ 07921, and (2) a telephone assigned call number **202-840-4914**, which information is stored at premises controlled by **T-MOBILE**, a wireless telephone service provider headquartered at 4 Sylvan Way, Parsippany, NJ, 07054. The information to be searched is described in the following paragraphs and in Attachment A. This affidavits is made in support of an application for search warrants under 18 U.S.C. § 2703(c)(1)(A) to require **VERIZON WIRELESS** and **T-MOBILE** to disclose to the government copies of the information further described in Section I of Attachment B, as to each telephone. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will

review the information to locate items described in Section II of Attachment B, as to each telephone.

2. I am a Special Agent with the Federal Bureau of Investigation and have been since May 2017. Prior to becoming an FBI Special Agent, Affiant was employed with the FBI as a Staff Operations Specialist in Washington D.C. and as a Surveillance Specialist in New York, New York since December 2012. I am currently assigned to the Pittsburgh Field Office, where the FBI is investigating the matters described below, along with members of the Pennsylvania State Police Western Regional Auto Theft Task Force (“WRATTTF”). Through the course of my training and experience, your Affiant has come to know that cellular telephones are regularly used during the course of criminal activity by individuals in order to communicate, coordinate, or sometimes execute their criminal conduct. My training and experience as an FBI Special Agent has made me familiar with the types of data that can be obtained from cellular telephones, to include data stored on the device as well as data available from cellular service providers. Your Affiant has used data retrieved from cellular telephone extracts and data provided by cellular service providers regularly as a part of, and to further, my investigations.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses involved in this investigation. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. Sections 371 (conspiracy), 2312 (interstate transportation of stolen motor vehicles) and 2314 (interstate transportation of stolen property) have been committed by Corey P. Pollard, Kirk L. Price and other persons not yet identified. There is also probable cause to search

the information described in Attachment A for evidence of these crimes as further described in Attachment B, as to each telephone.

PROBABLE CAUSE

5. The FBI is working with WRATTf in the investigation and prosecution of crimes associated with organized theft of vehicles, heavy equipment, landscaping equipment and all-terrain vehicles. The offenses have been committed in Pennsylvania, Delaware and Maryland.

6. The FBI and WRATTf are investigating approximately ten incidents between July of 2019 and January of 2020, involving vehicle and property thefts, and the related interstate transportation of those stolen items. Four of those incidents are described in more detail below.

7. The targets of this investigation are Corey P. Pollard and Kirk L. Price, both of whom were indicted in this District on January 28, 2020, and have been charged with offenses involving the four incidents described below.

8. Pollard and Price are both presently in the process of completing federal sentences stemming from convictions for drug offenses committed in Maryland. The instant investigation has revealed that they know each other and associate with each other. Specifically, investigators have found a photograph on Price's Instagram account depicting Price and Pollard together in a federal prison. Price and Pollard both reside in Maryland, and they were both recently supervised by United States Probation Officer Takiyah McWilson. Officer McWilson informed investigators in this case, approximately two weeks ago, that Pollard's cell phone number is 202-604-0663, and Price's cell phone number is 202-840-4914.

9. According to open source databases privileged to law enforcement, telephone number 202-604-0663 (Pollard's phone) is serviced by Verizon Wireless. According to open

source databases privileged to law enforcement, 202-840-4914 (Price's phone) is serviced by T-Mobile.

Incident # 1

10. On November 24, 2019, the Car Right dealership located in Moon Township Pennsylvania was victimized by a group consisting of at least five individuals. At approximately 2:00 a.m., the perpetrators gained entry to the business area of the dealership by removing the glass and trim from the door to the dealership. They subsequently found and took numerous sets of keys to vehicles on the premises, and then stole the following four vehicles which were part of Car Right's inventory for sale:

- (a) a 2018 Jeep Cherokee Trackhawk, bearing VIN ending in 4414, was stolen;
- (b) a 2019 Ram 1500, bearing VIN ending in 7845, was stolen;
- (c) a 2018 Ram 3500, bearing VIN ending in 6730, was stolen; and
- (d) a 2020 Ram 1500, bearing VIN ending in 5683, was stolen.

The approximate total retail value of these vehicles is \$272,700.

11. Car Right's video surveillance captured images of several of the perpetrators, all of whom were wearing heavy winter clothing and hats so as to conceal their physical appearances. The video shows that the perpetrators left the Car Right dealership property, with the four above-described vehicles, at approximately 4:07 a.m.

12. Investigators obtained video footage from cameras located at the intersection of University Boulevard and Beaver Grade Road, Moon Township, PA, which is approximately 0.9 miles away from Car Right. These videos show the four stolen vehicles being driven along the road at approximately 4:08 a.m., followed by a fifth vehicle. That fifth vehicle is an Infiniti automobile, bearing a Maryland license plate registered to Kirk L. Price.

13. Video footage obtained from a Sheetz store in Moon Township shortly after the thefts shows the five vehicles pulling into the Sheetz lot. Two of the vehicles' occupants entered the Sheetz store, and one of those men depicted in the video has been identified by investigators as Pollard.

14. Through GPS and other geo locator information, the investigators have been able to locate and recover all four of the stolen vehicles. Three of the vehicles were recovered in Maryland, and the fourth was recovered in Newark, Delaware, after it was abandoned by the perpetrators of a cell phone store burglary (see ¶ 16 below).

15. One of the vehicles recovered in Maryland was the 2020 Ram 1500 described above. This pickup truck was found two days after the Car Right theft, parked on Vine Street in Capitol Heights, Maryland, just outside the residence of Kirk L. Price.

Incident # 2

16. On December 5, 2019, the Verizon cell phone store located in the Suburban Plaza in Newark, Delaware, was burglarized at approximately 5:00 a.m. A sledge hammer was used to smash the glass entrance door. Thirty-nine cell phones, with an approximate value of \$22,483.00, were stolen.

17. Video surveillance footage from the scene outside the store shows that the perpetrators of the burglary had arrived at the scene in two separate vehicles. One of those vehicles was a Ram 1500 pickup, which was abandoned by the perpetrators after the burglary. That pickup was found parked a short distance from the Verizon store and was later identified by investigators as being the 2019 Ram 1500 that had been stolen from Car Right on November 24, 2019.

18. The second vehicle used by the perpetrators, as depicted in the surveillance video of the area outside the store, was a white Maserati. This vehicle's license plate was captured by a

different surveillance camera system in Newark, Delaware in the early morning hours of December 5, 2019. That license plate was registered to Corey Pollard, who is the registered owner of a white Maserati.

Incident # 3

19. In the early morning hours of December 15, 2019, the Susquehanna Ford dealership in Quarryville, PA was victimized by a burglary involving the thefts of a 2020 Ford F-150 Raptor pickup truck, and a 2020 Ford F-350 pickup truck.

20. Video from surveillance cameras in Howard County, approximately 72 miles from the dealership, depicts the two stolen vehicles being driven away from the direction of the dealership, as they are being led by a third vehicle, which was an Audi SUV. The license plate on the Audi SUV was registered to Enterprise Rent A Car, and Enterprise records were later examined by investigators. Those records show that the Audi SUV had been rented to Pollard on December 12, 2019, and then returned on December 15, 2019.

21. The F-150 and F-350 stolen from the Susquehanna Ford dealership were subsequently recovered in Maryland.

Incident # 4

22. On December 23, 2019, a dealership known as "Land Rover of the Main Line," located in Wayne, PA, was victimized. In this incident, at least seven perpetrators are believed to have been involved, as six Range Rovers, identified as follows, were driven away:

- (a) a 2020 Range Rover Sport, bearing VIN ending with 9327, was stolen;
- (b) a 2020 Range Rover, bearing VIN ending in 2211, was stolen;
- (c) a 2016 Range Rover Sport, bearing VIN ending in 9276, was stolen;
- (d) a 2017 Range Rover Sport, bearing VIN ending in 2495, was stolen;

- (e) a 2016 Range Rover HSE, bearing VIN ending in 5908, was stolen; and
- (f) a 2017 Range Rover HSI, bearing VIN ending in 1742, was stolen.

The approximate total retail value of these vehicles is \$550,000.

23. The 2016 Range Rover Sport was recovered in Accocreek, Maryland, in the same area where the Trackhawk from the Car Right incident was recovered. The 2017 Range Rover Sport was recovered on January 7, 2020 in Baltimore, Maryland. On January 9, 2020, the 2016 Range Rover HSE was recovered on Baltimore Avenue in Laurel, Maryland.

24. On January 21, 2020, police in Maryland located the 2020 Range Rover Sport, as it was being driven by Pollard. The officers arrested Pollard on a stolen property charge. At the time of the arrest, Pollard had two cell phones in the vehicle, which can be described as a white Apple iPhone with black case and a black Samsung phone in a black case.

PHONE DATA EVIDENCE

25. Based upon the foregoing, there is probable cause to conclude that the records and physical location data of the telephones with numbers 202-604-0663 and 202-840-4914 constitute evidence of crimes committed, and being committed, in the Western District of Pennsylvania and elsewhere. The records and physical location data, by itself and/or in conjunction with complementary investigative steps, will reflect where the telephones, Pollard, Price and their criminal associates were located when criminal activity occurred.

26. In my training and experience, I have learned that both **VERIZON WIRELESS** and **T-MOBILE** are companies that provide cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including cell-site data, also known as “tower/face information” or “cell tower/sector records.” Cell-site data identifies the “cell towers” (i.e., antenna towers covering

specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the “sector” (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate location of the cellular telephone but is typically less precise than other types of location information, such as E-911 Phase II data or Global Positioning Device (“GPS”) data.

27. Based on my training and experience, I know that **VERIZON WIRELESS** and **T-MOBILE** can collect cell-site data about the targeted telephones. I also know that wireless providers such as **VERIZON WIRELESS** and **T-MOBILE** typically collect and retain cell-site data pertaining to cellular phones to which they provide service in their normal course of business in order to use this information for various business-related purposes.

28. Based on my training and experience, I know that **VERIZON WIRELESS** and **T-MOBILE** also collect per-call measurement data, which **VERIZON WIRELESS** and **T-MOBILE** also refer to as the “real-time tool” (“RTT”). RTT data estimates the approximate distance of the cellular device from a cellular tower based on the speed with which signals travel between the device and the tower. This information can be used to estimate an approximate location range that is more precise than typical cell-site data.

29. Based on my training and experience, I know that wireless providers such as **VERIZON WIRELESS** and **T-MOBILE** typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless telephone service. I

also know that wireless providers such as **VERIZON WIRELESS** and **T-MOBILE** typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other communications sent or received by a particular phone and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because the information can be used to identify the target telephones' user or users and may assist in the identification of co-conspirators and/or victims.

AUTHORIZATION REQUEST

30. Based on the foregoing, I request that the Court issue the proposed search warrants, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

31. I further request that the Court direct **VERIZON WIRELESS** and **T-MOBILE** to disclose to the government with respect to each telephone, any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrants will be served on **VERIZON WIRELESS** and **T-MOBILE**, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrants at any time in the day or night.

32. I further request that the Court order that all papers in support of this application, including the affidavit and search warrants, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because

their premature disclosure may seriously jeopardize that investigation, including by giving targets an opportunity to destroy or tamper with evidence, change patterns of behavior, notify confederates, and flee from prosecution.

Respectfully Submitted,



Ryan Melder, SA, FBI

Subscribed and sworn to before
me on February 14, 2020



CYNTHIA R. EDDY
CHIEF UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A - 202-604-0663

Property to Be Searched

This warrant applies to records and information associated with the cellular telephone assigned call number **202-604-0663**, which information is stored at premises controlled by **VERIZON WIRELESS** (“the Provider”), headquartered at 180 Washington Valley Road, Bedminster, NJ 07921.

ATTACHMENT B – 202-604-0663

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the Pennsylvania State Police, the FBI and WRATTF the following information pertaining to the Account listed in Attachment A for the time period June 1, 2019 to present:

- a. The following information about the customers or subscriber of the Account:
 - i. Names (including subscriber names, user names, and screen names);
 - ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
 - iii. Local and long distance telephone connection records;
 - iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol (“IP”) addresses) associated with those sessions;
 - v. Length of service (including start date) and types of service utilized;
 - vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifier (“MEID”); Mobile Identification Number (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”); International Mobile Subscriber Identity Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”);
 - vii. Other subscriber numbers or identities (including the registration Internet Protocol (“IP”) address); and
 - viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.

- b. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Account, including:
 - i. the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and
 - ii. information regarding the cell tower and antenna face (also known as “sectors”) through which the communications were sent and received, as well as per-call measurement data (also known as the “real-time tool” or “RTT” data).

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence, fruits, contraband, and instrumentalities of violations of 18 U.S.C. §§ 371, 2312 and 2314 involving Corey P. Pollard, Kirk L. Price and others during the period June 1, 2019 to the present.

ATTACHMENT A - 202-840-4914

Property to Be Searched

This warrant applies to records and information associated with the cellular telephone assigned call number **202-840-4914**, which information is stored at premises controlled by **T-MOBILE** (“the Provider”), headquartered at 4 Sylvan Way, Parsippany, NJ 07054.

ATTACHMENT B – 202-840-4914

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the Pennsylvania State Police, the FBI and WRATTF the following information pertaining to the Account listed in Attachment A for the time period June 1, 2019 to present:

- a. The following information about the customers or subscriber of the Account:
 - i. Names (including subscriber names, user names, and screen names);
 - ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
 - iii. Local and long distance telephone connection records;
 - iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol (“IP”) addresses) associated with those sessions;
 - v. Length of service (including start date) and types of service utilized;
 - vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifier (“MEID”); Mobile Identification Number (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”); International Mobile Subscriber Identity Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”);
 - vii. Other subscriber numbers or identities (including the registration Internet Protocol (“IP”) address); and
 - viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.

- b. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Account, including:
 - i. the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and
 - ii. information regarding the cell tower and antenna face (also known as “sectors”) through which the communications were sent and received, as well as per-call measurement data (also known as the “real-time tool” or “RTT” data).

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence, fruits, contraband, and instrumentalities of violations of 18 U.S.C. §§ 371, 2312 and 2314 involving Corey P. Pollard, Kirk L. Price and others during the period June 1, 2019 to the present.